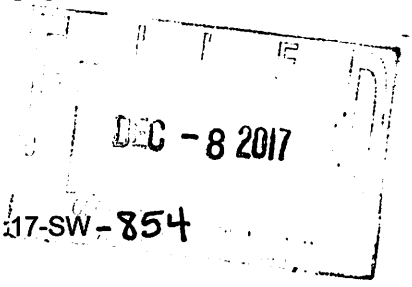
AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched

9486 James Madison Hwy., Warrenton, VA 20187
(Target Location #1)

Case No. 1:17-SW-854

Inc.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC §§ 841(a)(1), 846, 18 USC §§ 1956(a)(1), 1956(h), 1960(a), 31 USC §§ 5324(a)(3) and 5324(d)	Conspiracy to distribute controlled substances, Laundering of monetary instruments, Operations of an unlicensed money transmitting business and Structuring of financial transactions

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Katherine Rumbaugh

Applicant's signature

Jason R. Clark, DEA/HSI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/8/17

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The properties to be searched are the following, including any and all structures and/or vehicles located within the curtilage thereof:

- 9486 James Madison Hwy, Warrenton, Virginia 20187 (Target Location #1)

Target Location #1 is a Valero Gas station. It is a single-story commercial building with a teal roof and yellow and white trim.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

All items constituting evidence and/or instrumentalities of violations of 21 U.S.C. §§ 841(a) and 846 (conspiracy to distribute a controlled substance); and all items constituting evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1956(a)(1) and 1956(h) (conspiracy to launder monetary instruments), 18 U.S.C. § 1960 (operating an unlicensed money transmitting business) and 31 U.S.C. §§ 5324(a)(3) and 5324(d) (structuring financial transactions to avoid reporting requirements); including but not limited to the following:

1. Controlled substances and/or controlled substances residue, indicia of distribution (such as scales or packaging materials), records and documents, receipts, notes ledgers, and other papers including any computerized or electronic records, including cellular telephones, relating to the ordering, purchase, or possession of controlled substances;

2. Records and documents, receipts, notes ledgers and other papers including any computerized or electronic records including cellular telephones, relating to the laundering of money or structuring of financial transactions;

3. United States currency, financial instruments — including but not limited to stocks and bonds — and other illicit gains;

4. Address and/or telephone books, appointment logs, daily or monthly planners, Rolodexes, meeting schedules, any and all materials reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, including any individuals with whom a financial relationship exists, as well as financial institutions and other individuals or businesses with whom a financial relationship exists;

5. Photographs, including still photos, negatives, video tapes, films, undeveloped film

and the contents therein, in particular photographs of co-conspirators, of assets and/ or controlled substances;

6. Indicia of occupancy, residency, rental and/ or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchases or lease agreements, and keys;

7. Tickets, notes, receipts, and other items relating to domestic and international travel, including but not limited to, airline tickets, boarding passes, airline receipts, car rental agreements, commercial bus tickets, passports, and visas;

8. Any locked or closed containers including but not limited to safes, both combination and lock type, and their contents, which could include any of the above listed evidence;

9. Books and records of corporations, partnerships, trusts and/or businesses, both domestic and foreign, including but not limited to: articles of incorporation or other formation or dissolution documents, bylaws, minutes of any corporate, board or shareholder meeting, stock registers or other records identifying corporate shareholders, records reflecting the true or beneficial owner of any business, documentation evidencing the secreting, movement, transfer, or conversion of assets, both monetary and non-monetary, records identifying shareholders, partners, directors, or officers, personnel or payroll records, income or excise tax returns and/or copies, corporate seals, financial statements, journals, ledgers, notes, workpapers, real estate transaction records, bank statements and related records, brokerage account statements and related records, cancelled checks, deposit slips and other items, withdrawal slips and other items, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, receipts, invoices, lease agreements, correspondence, agreements,

declarations, certifications, powers-of-attorney and other items evidencing the ownership or control of other business entities, and other items evidencing income, expenditures, assets, liabilities or investments;

10. Books and records of personal income, expenditures or investments, both domestic and foreign, including but not limited to: income or excise tax returns and/or copies, financial statements, journals, ledgers, notes, workpapers, bank statements and related records, cancelled checks, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, brokerage or other financial institution transaction statements, stocks, bonds, mortgages, real estate transaction records, receipts, invoices, and other items evidencing income, expenditures, assets, liabilities or investments;

11. Records of loans, contracts, mortgages, notes, agreements, applications, schedules, records of payments, financing statements, collateral records, and other financial records;

12. Records relating to the use of landline, credit card, and cellular telephone services, including cellular telephones, facsimile machines and the stored electronic communications therein, as well as documentation containing telephone, credit card, and computer access codes;

13. Records relating to the rental of post office boxes or drop boxes, domestic and foreign;

14. All documents reflecting the names of personal aliases, corporate entities, shell corporations, partnerships, relatives and associates (nominees);

15. Logs of electronic communications, disks of communications, hard copies of communications, audio cassette tapes of communications, calendars, appointment books, telephone number lists, incoming and outgoing facsimile messages, and any documentation, telephone records, bank account information or wire transfer information;

16. All of the above relative to at least the following individuals and/or corporations or business entities or their co-conspirators:

a. Nasser Latif, a.k.a. "John Latif"
b. Nader Noori-Moghaddam, a.k.a. "Hulk"
c. Nah Partners Inc.
d. Nader & Nader LLC

17. Electronic equipment, including but not limited to computers, facsimile machines, currency counting machines, telephone answering machines used to generate, transfer, count, record, and/or store the information described in the above-listed evidence. Additionally, computer software, tapes, discs, audio tapes, flash drives, memory sticks, PDAs, cellular telephones, and the contents therein, containing the information generated by the aforementioned electronic equipment.

18. For any computer or storage medium whose seizure if otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow otherw to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;

d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records or or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

19. As used above, he terms "records" and "information" includes all forms of creation

or storage, including any orm of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

20. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

21. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF	)	
	)	UNDER SEAL
9486 James Madison Hwy., Warrenton, VA 20187 (Target Location #1)	)	No. 1:17-SW-854

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH AND SEIZURE WARRANTS

I, Jason R. Clark, Detective with the Fauquier County Sheriff's Office, Task Force Officer with the Drug Enforcement Agency and Homeland Security Investigations, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer with the United States Drug Enforcement Administration (DEA) as well as Homeland Security Investigations (HSI) and have been so employed for approximately one year. I am also employed as a Narcotics Detective with the Fauquier County Sheriff's Office and have been so employed since November 2016. I was previously employed as a Detective with the Culpeper County Sheriff's Office from 2011 to 2016, and before that, worked for the Spotsylvania County Sheriff's Office from 2002 to 2011. While employed as a Detective with the Culpeper Sheriff's Office, I also worked as a Task Force Officer with the DEA's Richmond, Virginia office for approximately three years. As a Task

Force Officer with DEA and HSI, I am authorized to conduct investigations into violations of the Controlled Substances Act and Controlled Substances Analogue Act. I have been involved in a variety of investigations into offenses ranging from simple possession of narcotics to complex conspiracies.

2. During my career in law enforcement, I have received training and experience in interviewing and interrogation techniques, arrest procedures, search and seizure, narcotics investigations, search warrant applications, and investigations of various other crimes. In the course of my training and experience, I have become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies. In the course of conducting these investigations, I have been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses; conducting physical surveillance; supporting undercover operations; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification system data; conducting court-authorized electronic surveillance; and preparing and executing search warrants that have led to seizures of narcotics, firearms, and other contraband.

3. Through instruction and participation in investigations, I have become familiar with the manner in which narcotics traffickers conduct their illegal business, and the methods used to disguise narcotics activities and launder the proceeds therefrom. For example, I know that individuals involved in drug distribution often use concealment compartments located within vehicles, furniture, and homes, which are used to conceal controlled substances, cash, and other contraband from law enforcement.

4. I submit this affidavit in support of an application for a search warrant for the following locations, and any and all structures and/or vehicles within the curtilage thereof, (collectively, the "**TARGET LOCATIONS**"), all of which are located within the Eastern District of Virginia:

a. 9486 James Madison Hwy, Warrenton, Virginia 20187 (**Target Location #1**)

b. 8299 Shimmering Rock Dr., Gainesville, Virginia 20155 (**Target Location #2**)

c. 8 Century St., Stafford, Virginia 22554 (**Target Location #3**)

The TARGET LOCATIONS are described in Attachment A, and the items to be seized are described in Attachment B.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. All observations that were not made personally by me were related to me by the persons who made the observations. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that NASSER LATIF and NADER NOORI-MOGHADDAM, and others, both known and unknown, have engaged and are continuing to engage in a conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846; a conspiracy to launder money, in violation of 18 U.S.C. §§ 1956(a)(1) and 1956(h); the operation of an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); and the structuring of financial transactions to evade reporting requirements, in violation of 31 U.S.C. §§ 5324(a)(3) and 5324(d). I further submit that the premises described in Attachment A

contain evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

PROBABLE CAUSE

7. **Target Location #1** is a Valero Gas station owned and operated by Nasser A. LATIF, a.k.a. "John Latif," and Nader NOORI-Moghaddam, a.k.a. "Hulk," by and through the business name NAH PARTNERS Inc. Public records list LATIF as the President and NOORI as the Secretary of NAH PARTNERS, which was incorporated and registered on or about October 6, 2004. Public records also list LATIF as the registered agent for NAH PARTNERS, and the company's listed address is **Target Location #2**, which is also LATIF's residence, as verified by law enforcement databases.

I. Purchases of Controlled Substances at Target Location #1

8. Multiple confidential sources, as well as members of the public, have reported to law enforcement that LATIF and NOORI are selling synthetic cannabinoids, commonly referred to as "Spice" or "K2," from the Valero Gas station at Target Location #1, on an ongoing basis. Subsequent investigation revealed that in and around July 2012, state law enforcement went to Target Location #1 and advised LATIF and NOORI that the synthetic cannabinoids they were selling — openly, at the time — were illegal, and that they should cease selling the product.

9. On or about April 3, 2017, law enforcement conducted a controlled buy at Target Location #1 using a confidential informant ("CI-1"). CI-1 purchased a silver Ziploc-style pouch bearing a picture of the cartoon character Scooby Doo for $53 from LATIF. Based on my training and experience, I know that "Scooby Snax" is a common name for synthetic cannabinoids. During the exchange, LATIF reached under the counter at the front of the Valero Gas station to retrieve the pouch, and then placed it in a brown paper bag, which he gave to CI-1.

LATIF placed the $53 in cash into the gas station's regular cash register, thereby commingling the proceeds with the business's legitimate profits. The silver pouch was seized; it contained approximately five grams of FUB-AKB48, a Schedule I controlled substance.

10. On or about April 10, 2017, law enforcement conducted another controlled buy at Target Location #1 using another confidential informant ("CI-2"). CI-2 went inside the Valero Gas station and asked for "spice" from "Hulk" (*i.e.*, NOORI). NOORI sold CI-2 silver Ziploc-style pouch bearing a picture of the cartoon character Scooby Doo for $53. During the exchange, NOORI reached under the counter at the front of the Valero Gas station to retrieve the pouch; NOORI also told CI-2 not to smoke too much of it. NOORI placed the $53 in cash into the gas station's cash register. The silver pouch was seized; it contained approximately five grams of AB-FUBINACA, a Schedule I controlled substance.

11. On or about May 25, 2017, law enforcement conducted another controlled buy at Target Location #1 using an undercover officer ("UC-1"). UC-1 went inside the Valero Gas station and asked "Hulk" (NOORI) to purchase some synthetic cannabinoids. NOORI sold UC-1 two silver Ziploc-style pouches, one bearing a picture of Scooby Doo, and one bearing the name "Diablo," for $106. During the exchange, NOORI reached under the counter at the front of the Valero Gas station to retrieve the pouches to give to UC-1. NOORI placed the $106 in cash into the gas station's cash register. One pouch contained approximately five grams of AB-FUBINACA, a Schedule I controlled substance. The other pouch contained approximately five grams of 5-Fluoro-AMB, a Schedule I controlled substance.

12. On or about September 14, 2017, law enforcement conducted another controlled buy at Target Location #1 using UC-1. UC-1 went inside the Valero Gas station and asked "John" (LATIF) for grape-flavored synthetic drugs. LATIF sold UC-1 two silver Ziploc-style

pouches, one labeled "BIZARRO," and the other labeled "24 MONKEY," for $74.20. As with prior exchanges, LATIF retrieved the pouches from under the counter, and then placed the cash payment in the business's cash register. The pouch labeled "BIZARRO" contained approximately one gram of 5-Fluoro-ADB, a Schedule I controlled substance. The pouch labeled "24 MONKEY" contained approximately one gram of a combination of 5-Fluoro-ADB, a Schedule I controlled substance, and FUB-AMB, a controlled substances analogue.

13. On or about November 20 and 21, 2017, law enforcement conducted two additional controlled buys at Target Location #1 using UC-1, one from LATIF and one from NOORI. On each occasion, UC-1 asked the target to purchase synthetic drugs, and on both occasions, the target sold UC-1 a substance packaged and labeled in the same manner as each of the prior controlled buys. On both occasions, the target placed the cash payment in the business's cash register. Lab results of the substances purchased November 20 and 21 are still pending.

II. Suspicious Shipping Activities to Target Locations #2 and #3

14. Virginia Department of Motor Vehicle records show that **Target Location #2** is LATIF's residence, and that **Target Location #3** is NOORI's residence.

15. Through surveillance of **Target Location #2** (LATIF's residence) law enforcement observed that packages have been shipped to Target Location #2 in a manner consistent with the mailing of synthetic drugs. Specifically, numerous packages delivered to Target Location #2 have originated from Hangzhou, China. Based on my training, education, and experience, I know that China is a common origin of supply for synthetic cannabinoids and other designer drugs.

16. Additionally, shipping records associated with **Target Location #3** (NOORI's residence) revealed that packages have been shipped to Target Location #3 in a manner

consistent with the mailing of synthetic drugs. Specifically, numerous packages delivered to Target Location #3 have originated from China, and the weights of the packages listed on the shipping records did not match the items described inside the package. For example, records for one package described it as a "key"; the package weight was approximately two pounds. Based on my training, education, and experience, I know that individuals involved in distributing controlled substances through the mail will commonly conceal their contraband by describing the shipments as innocuous items.

17. In the course of conducting surveillance on Target Location #1, law enforcement has observed both LATIF and NOORI engaging in the same pattern of behavior when opening and closing the gas station at Target Location #1. Namely:

a. The target arrives at Target Location #1 in the morning and parks his vehicle immediately adjacent to the front door. The target opens the gas station and then unloads the vehicle, then moves the vehicle to a space close to the road.

b. When closing the store, the target retrieves the vehicle from the road and parks it immediately adjacent to the front door. The target then loads the vehicle, locks up the gas station, and then drives away.

18. Based on my training, experience, and knowledge of this investigation, I believe that both LATIF and NOORI are having synthetic cannabinoids shipped to their respective homes (Target Locations #2 and #3). I further believe that LATIF and NOORI are storing the synthetic cannabinoids at Target Locations #2 and #3 when the gas station is closed in order to avoid the contraband being stolen.

III. Suspicious Financial Activities of NAH PARTNERS and NOORI

19. In addition to the ongoing sale of synthetic cannabinoids, as set forth above, investigators have learned that NAH PARTNERS has also operated a check-cashing business out of the Valero Gas station at Target Location #1 since at least in and around 2008. However, this business did not register as a money transmitting business until in and around May 2016.

20. Bank records for a Middleburg Bank account in the name of NAH PARTNERS reveal a total of $255,000 in structured cash withdrawals, in amounts below the reporting threshold of 31 U.S.C. § 5313(a), between in and around October 2016 through in and around January 2017. Specifically:

a. Between on or about October 3, 2016, and on or about November 21, 2016, there were approximately thirteen withdrawals of $10,000 spaced out every two to seven days.

b. Between on or about November 21, 2016, and on or about December 8, 2016, there were approximately six withdrawals of $5,000, spaced out every two to three days. On or about December 5, 2016, two separate $5,000 withdraws occurred on the same day.

c. On or about December 9, 2016, a withdrawal for $10,000 occurred. Then, between on or about December 14, 2016, and on or about January 12, 2017, there were approximately seven withdrawals of $5,000 spaced out every two to three days. On or about December 23, 2016, two separate $5,000 withdraws occurred on the same day.

d. On or about January 13 and 17, 2017, two withdrawals were conducted for $10,000 each. Between on or about January 18, 2017, and on or about January 26, 2017, there were approximately four withdrawals of $5,000 spaced out every two to three days.

e. On or about January 31, 2017, another withdrawal for $10,000 occurred.

21. As discussed above, LATIF is the registered agent for Nah Partners. LATIF's email address is ali.l@yahoo.com.

22. Additionally, bank records for NOORI reveal a series of monetary transfers to and from NOORI's personal account, indicative of money laundering activities and structured financial transactions. Specifically:

a. Between in and around November 15, 2016, and June 16, 2017, there were thirty-one cash deposits totaling approximately $137,440 made to NOORI's personal account. The deposits were made in amounts ranging from approximately $190 to $12,000 by individuals in eleven different states.

b. On or about December 5, 2016, a $400,000 cashier's check was deposited in NOORI's account with the remitter Nader & Nader LLC. Based on publicly available information, Nader & Nader LLC holds itself out as an Iranian art dealer based in New York City.

c. On or about June 9, 2017, a $38,000 check drawn on a Bank of America account and bearing no other identifying information was deposited to NOORI's account.

d. Between in and around December 12, 2016, and June 13, 2017, there were multiple outgoing transfers from NOORI's account (wire transfers, outgoing checks, and other withdrawals) totaling approximately $386,535. Most of the transfer recipients were apparently unrelated individuals located in different parts of the United States. Additionally, a number of the outgoing transfers involved separate checks written to the same individual on the same day, for example:

i. On or about December 12, 2016, NOORI wrote three checks to K.R. in amounts of $9,000, $9,000, and $8,350.

ii. On or about December 24, 2016, NOORI wrote four checks to K.M. in amounts of $5,000 each, totaling $20,000.

iii. On or about December 24, 2016, NOORI wrote two checks to H.K. for $5,000 each, totaling $10,000.

iv. On or about December 26, 2016, NOORI wrote two checks to N.A. for $11,633 each, totaling $23,266.

e. Additionally, in and around the same time frame, there were approximately fifteen structured cash withdrawals from NOORI's account. The cash withdrawals were made from locations in Virginia and ranged in amounts from $500 to $9,000, below the reporting threshold of 31 U.S.C. § 5313.

23. The email address affiliated with NOORI's personal bank account, which is associated with the foregoing transactions, is naderdady@yahoo.com.

24. Upon information and belief, NOORI has not registered as a money transmitting service with FinCen in accordance with 31 U.S.C. § 5330.

EVIDENCE AT THE PREMISES TO BE SEARCHED

25. Given the evidence and circumstances discussed in this affidavit, there is reason to believe that evidence related to a conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846; a conspiracy to launder money, in violation of 18 U.S.C. §§ 1956(a)(1) and 1956(h); the operation of an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960; and the structuring of transactions to evade reporting requirements, in violation of 31 U.S.C. § 5324, will be found within the Target Locations.

Specifically, there is probable cause to believe that LATIF and NOORI, who exercise control over the Target Locations, are actively involved in the foregoing offenses, and maintain within the Target Locations items related to such conduct.

26. This conclusion is further supported by my experience, training, and knowledge of this investigation as related to the distribution of controlled substances, through which I am aware of the following information:

a. Drug traffickers commonly maintain at their residences and on their property additional quantities of the illicit drugs being distributed, as well as packaging materials, scales, owe sheets, and other drug paraphernalia in their residences or on their property. Such contraband may be concealed in locations known to the traffickers to avoid law enforcement detection.

b. Drug traffickers commonly maintain at their residences and on their property books, records, receipts, mobile data storage units, computers, notes, ledgers, airline tickets, money orders, passports, visas, and other papers relating to the transportation, purchase, packaging, sale, and distribution of controlled substances.

c. Drug traffickers commonly maintain in their residences and on their property books, paper, and other records which reflect the names, addresses, and telephone numbers of their suppliers, couriers, customers, and other associates in the illegal drug trade.

d. Drug traffickers commonly maintain books, papers, and documents in secure locations within their residences and their property, so they can have ready access to such information, including documents related to their rental or occupancy of their residence and financial records. These financial records include receipts, wire transfers,

money orders that aid in the concealment and transfer of proceeds from their illicit drug trade.

e. Drug traffickers attempt to legitimize the proceeds from the sale of controlled substances. Books and papers relating to such efforts, including cashier checks, money orders, and ledgers are maintained in the residences and on the property of the drug trafficker. Drug traffickers often keep information and/or currency relating to their illicit drug trade in locked or closed containers in their residence in an attempt to secure these items.

f. Drug traffickers take, or cause to be taken, photographs and/or videos of themselves, their associates in the drug trade, property derived from the distribution of narcotics, and their products, and that such photographs and/or videos are often kept in their residences.

g. Drug traffickers commonly make attempts to conceal contraband in vehicles for the purpose of transportation.

h. Drug traffickers very often place assets, including real and personal property, such as vehicles, in names other than their own to avoid the detection and forfeiture of such assets by government agencies and continue to use these assets and to exercise dominion and control over them even though the assets are normally owned by them.

27. Furthermore, based on my experience, training, and knowledge of this investigation as it relates to financial crimes, including money laundering and/or structured financial transactions, I am aware of the following information:

a. It is common for individuals involved in financial crimes to hide the

proceeds and records of such financial crimes — including but not limited to books, records, receipts, notes, ledgers, business and personal checks, business and individual checking account and brokerage account statements, credit cards, credit card statements, account numbers, access numbers, and false identifications — within their residences and offices/businesses, for ready access and also to conceal such items from law enforcement. These individuals will often deposit monies derived from an illegal activity into bank or brokerage accounts that they maintain, and then use those monies through wire transfers and other withdrawals and checks written from the accounts.

b. Individuals engaging in financial crimes such as money laundering and structuring transactions will commonly convert the proceeds from unlawful activities into other assets such as real property, investments, automobiles, boats, and aircraft. I also know that it is a common practice of individuals involved in money laundering to maintain at their residences, places of business, and other sites to which they have access, records such as (1) corporate and accounting records, (2) telephone bills and statements, (3) banking, brokerage, and investment files and records, and (4) correspondence with co-conspirators which are related to their illegal activities.

c. Individuals engaged in financial crimes often conceal large amounts of currency, financial instruments, precious metals, jewelry and other things of value and/or proceeds of financial transactions made from engaging in financial crimes within their residences, offices/businesses, garages, storage buildings, automobiles, and safety deposit boxes.

d. Money service businesses, whether licensed or not, necessarily require the production and retention of records on the business premises and/or in the personal

residences indicative of the acquisition and disposition of large sums of currency and/or currency equivalents. The records produced and retained include the types of records identified in Attachment B, which is incorporated herein.

28. I also know through my training, experience, and knowledge of this investigation, that it is common to maintain and store the aforementioned evidence, in particular of financial crimes, electronically, using computer hardware, software, electronic storage devices, and different types of computer media, as discussed more fully below.

ELECTRONIC EVIDENCE

29. Pursuant to Rule 41(e)(2)(B), the warrant applied for would also authorize the seizure, or, potentially, the copying, of electronically stored information within any seized digital devices and electronic storage media. As used herein, the terms "electronic storage media" and digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

30. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found

in the subject premises, there is probable cause to believe that the records and information described in Attachment B will be stored in such media or devices for, but not limited to, the following reasons:

a. Individuals who engage in criminal activities, in particular financial crimes, use digital devices to communicate with co-conspirators online, but they also store on computer hard drives and other electronic storage media records relating to their illegal activity. Online criminals store these documents and records, which can include logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things:

i. keep track of co-conspirators' contact information;

ii. keep a record of illegal transactions for future reference;

iii. keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and

iv. store stolen data for future exploitation.

b. Individuals engaging in the criminal activites, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media — in particular, computers' internal hard drives — contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser

typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the seized items were used, the purpose of their use, who used them, and when. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the Target Locations because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in

use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

e. I know that when an individual uses a digital device to engage in criminal activities, including criminal conspiracies, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of

how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

32. *Methods to be used to search digital devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from electronic storage media also requires specialized

tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not able to be segregated from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files;

however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever

increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in

advance of the forensic examination of the media or devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

34. Based on the information discussed above, the specific items to be seized are described and detailed in Attachment B to the respective search warrant applications.

CONCLUSION

35. Based on the information provided in this affidavit, I submit that there is probable cause to believe that the items set forth in Attachment B will be found within the Target Locations, as described in Attachment A, and that such items constitute evidence related to the possession of controlled substances with intent to distribute, laundering of monetary instruments, structuring of financial transactions, and any attempts and/or conspiracies to do the same, in violation of 21 U.S.C. §§ 841(a)(1) and 846, 18 U.S.C. §§ 1956(a)(1) and 1956(h), 18 U.S.C. § 1960, and 31 U.S.C. §§ 5324(a)(3) and 5324(d).

36. Wherefore, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I respectfully request warrants to search the TARGET LOCATIONS, which are all located within the Eastern District of Virginia.

37. I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

Jason R. Clark
Fauquier County Sheriff's Detective
DEA / HSI Task Force Officer

Sworn and subscribed to me this 8th day of December, 2017.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

The Honorable Theresa Carroll Buchanan
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The properties to be searched are the following, including any and all structures and/or vehicles located within the curtilage thereof:

- 9486 James Madison Hwy, Warrenton, Virginia 20187 (Target Location #1)

Target Location #1 is a Valero Gas station. It is a single-story commercial building with a teal roof and yellow and white trim.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

All items constituting evidence and/or instrumentalities of violations of 21 U.S.C. §§ 841(a) and 846 (conspiracy to distribute a controlled substance); and all items constituting evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1956(a)(1) and 1956(h) (conspiracy to launder monetary instruments), 18 U.S.C. § 1960 (operating an unlicensed money transmitting business) and 31 U.S.C. §§ 5324(a)(3) and 5324(d) (structuring financial transactions to avoid reporting requirements); including but not limited to the following:

1. Controlled substances and/or controlled substances residue, indicia of distribution (such as scales or packaging materials), records and documents, receipts, notes ledgers, and other papers including any computerized or electronic records, including cellular telephones, relating to the ordering, purchase, or possession of controlled substances;

2. Records and documents, receipts, notes ledgers and other papers including any computerized or electronic records including cellular telephones, relating to the laundering of money or structuring of financial transactions;

3. United States currency, financial instruments — including but not limited to stocks and bonds — and other illicit gains;

4. Address and/or telephone books, appointment logs, daily or monthly planners, Rolodexes, meeting schedules, any and all materials reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, including any individuals with whom a financial relationship exists, as well as financial institutions and other individuals or businesses with whom a financial relationship exists;

5. Photographs, including still photos, negatives, video tapes, films, undeveloped film

and the contents therein, in particular photographs of co-conspirators, of assets and/ or controlled substances;

6. Indicia of occupancy, residency, rental and/ or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchases or lease agreements, and keys;

7. Tickets, notes, receipts, and other items relating to domestic and international travel, including but not limited to, airline tickets, boarding passes, airline receipts, car rental agreements, commercial bus tickets, passports, and visas;

8. Any locked or closed containers including but not limited to safes, both combination and lock type, and their contents, which could include any of the above listed evidence;

9. Books and records of corporations, partnerships, trusts and/or businesses, both domestic and foreign, including but not limited to: articles of incorporation or other formation or dissolution documents, bylaws, minutes of any corporate, board or shareholder□s meeting, stock registers or other records identifying corporate shareholders, records reflecting the true or beneficial owner of any business, documentation evidencing the secreting, movement, transfer, or conversion of assets, both monetary and non-monetary, records identifying shareholders, partners, directors, or officers, personnel or payroll records, income or excise tax returns and/or copies, corporate seals, financial statements, journals, ledgers, notes, workpapers, real estate transaction records, bank statements and related records, brokerage account statements and related records, cancelled checks, deposit slips and other items, withdrawal slips and other items, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, receipts, invoices, lease agreements, correspondence, agreements,

declarations, certifications, powers-of-attorney and other items evidencing the ownership or control of other business entities, and other items evidencing income, expenditures, assets, liabilities or investments;

10. Books and records of personal income, expenditures or investments, both domestic and foreign, including but not limited to: income or excise tax returns and/or copies, financial statements, journals, ledgers, notes, workpapers, bank statements and related records, cancelled checks, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, brokerage or other financial institution transaction statements, stocks, bonds, mortgages, real estate transaction records, receipts, invoices, and other items evidencing income, expenditures, assets, liabilities or investments;

11. Records of loans, contracts, mortgages, notes, agreements, applications, schedules, records of payments, financing statements, collateral records, and other financial records;

12. Records relating to the use of landline, credit card, and cellular telephone services, including cellular telephones, facsimile machines and the stored electronic communications therein, as well as documentation containing telephone, credit card, and computer access codes;

13. Records relating to the rental of post office boxes or drop boxes, domestic and foreign;

14. All documents reflecting the names of personal aliases, corporate entities, shell corporations, partnerships, relatives and associates (nominees);

15. Logs of electronic communications, disks of communications, hard copies of communications, audio cassette tapes of communications, calendars, appointment books, telephone number lists, incoming and outgoing facsimile messages, and any documentation, telephone records, bank account information or wire transfer information;

16. All of the above relative to at least the following individuals and/or corporations or business entities or their co-conspirators:

a. Nasser Latif, a.k.a. "John Latif"
b. Nader Noori-Moghaddam, a.k.a. "Hulk"
c. Nah Partners Inc.
d. Nader & Nader LLC

17. Electronic equipment, including but not limited to computers, facsimile machines, currency counting machines, telephone answering machines used to generate, transfer, count, record, and/or store the information described in the above-listed evidence. Additionally, computer software, tapes, discs, audio tapes, flash drives, memory sticks, PDAs, cellular telephones, and the contents therein, containing the information generated by the aforementioned electronic equipment.

18. For any computer or storage medium whose seizure if otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow otherw to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;

d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records or or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

19. As used above, he terms "records" and "information" includes all forms of creation

or storage, including any orm of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

20. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

21. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.